Table of Contents
Statewide Information Security Manual

Chapter 1 – Classifying Information and Data
Section 1 – Setting Classification Standards

Chapter 2 – Controlling Access to Information and Systems
Section 1 – Controlling Access to Information and Systems

Chapter 3 – Processing Information and Documents
Section 1 – Networks
Section 2– System Operations and Administration
Section 3– E-mail and the Worldwide Web
Section 4 – Telephones & Fax
Section 5 – Data Management
Section 6– Backup, Recovery and Archiving
Section 7– Document Handling
Section 8– Securing Data
Section 9– Other Information Handling and Processing

Chapter 4– Purchasing and Maintain ing Commercial Software
Section 1 – Purchasing and Installing Software Section 2– Software Maintenance & Upgrade
Section 3– Other Software Issues

Chapter 5– Securing Peripherals and Other Equipment
Section 1 – Purchasing and Installing Hardware
Section 2– Cabling, UPS, Printers and Modems
Section 3– Consumables
Section 4– Working Off Premises or Using Outsourced Processing
Section 5– Using Secure Storage
Section 6– Documenting Hardware
Section 7– Other Hardware Issues

Chapter 6 – Combating Cyber Crime
Section 1 – Combating Cyber Crime

Chapter 7 – Controlling E-Commerce Information Security
Section 1 – E-Commerce Issues

Chapter 8– Developing and Maintaining In-House Software
Section 1 – Controlling Software Code
Section 2 – Software Development
Section 3 – Testing & Training
Section 4 – Documentation
Section 5 – Other Software Development

Chapter 9– Dealing with Premises Related Considerations
Section 1 – Premises Security
Section 2 – Data Stores
Section 3 – Other Premises Issues

Chapter 10 – Addressing Personnel Issues Relating to Security
Section 1 – Contractual Documentation
Section 2 – Confidential Personnel Information
Section 3 – Personnel Information Security Responsibilities
Section 4 – HR Management
Section 5 – Staff Leaving Employment
Section 6 – HR Issues Other

Chapter 11 – Delivering Training and Staff Awareness
Section 1 – Awareness
Section 2 – Training

Chapter 12 – Complying with Legal and Policy Requirements
Section 1 – Complying with Legal Obligations
Section 2 – Complying with Policies
Section 3 – Avoiding Litigation
Section 4 – Other Legal Issues

Chapter 13 – Detecting and Responding to IS Incidents
Section 1 – Reporting Information Security Incidents
Section 2 – Investigating Information Security Incidents
Section 3– Corrective Activity Section 4– Other Information Security Incident Issues

Chapter 14 – Planning for Business Continuity
Section 1 – Business Continuity Management (BCM)